CLAIMS

What is claimed is:

1. A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server;

verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufactured of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server; and

inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device.

2. The method of Claim 1, wherein said non-public, secure value is a secret number (secret) and said method further comprises forwarding a first copy of said secret via a secure communication medium to said credential server.

3. The method of Claim 2, further comprising:

hashing a second copy of said secret with a public key from said endorsement key pair;

combining a first hash result from said hashing step with the public key to create the endorsement key (EK); and

forwarding said EK to said credential server to initiate a credential process.

4. The method of Claim 3, said verifying step further comprising:

receiving said EK from said device at the credential server;

hashing the public key within the received EK with the first copy of said secret received during said forwarding step to provide a second hashed value;

comparing the first hashed value from within the EK with the second hash value; and

confirming said EK is from a valid device when said comparing step results in a match.

5. The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. The method of Claim 1, wherein said value is injected into said device, and said value is a single-use parameter, said method further comprising immediately destroying said value within said device following a creation of said EK.

8. The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises communicating said value from said device to said credential server via a secure communication medium.

9. The method of Claim 1, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices.

10. The method of Claim 1, wherein said device is a trusted platform module (TPM).

11. A TPM device manufactured and authenticated according to the steps of Claim 1.

12. A data processing system comprising:

a processor;

a trusted platform module (TPM) chip;

a bus for interconnecting said processor and said TPM chip;

a network interface with communication means for connecting said TPM to a secure credential server; and

means, whereby said TPM is able to verify an endorsement key pair as being a valid pair generated within said TPM by utilizing a secure, private, single-use value inserted by a TPM vendor into the TPM during manufacture of the TPM.

13. The data processing system of Claim 12, wherein said means for verifying an endorsement key pair further comprises:

means for packaging a public value of said endorsement key pair and a hash of said value into an endorsement key (EK); and

means for forwarding said EK to said credential server, wherein said credential server returns an endorsement certificate only when the EK was generated within the TPM as confirmed by a comparison of the hashed value with a calculated hashed value at the credential server.

14. A data processing system utilized for issuing endorsement certificates, comprising:

a processor;

a memory couple to said processor via an interconnect;

a security mechanism for ensuring optimum security of processes within said data processing system;

input/output mechanism for receiving a first value received from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and

secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key and a second value provided for verifying that said EK was generated from within one of said manufactured TPM devices ; and

program means for determining, by utilizing said second value, when said EK is a valid EK of an endorsement key pair that was generated within one of said manufactured TPM devices.

15. The data processing system of Claim 14, further comprising means for generating a certificate only when said EK is determined to be a valid EK.

16. The data processing system of Claim 14, further comprising:

recording when a request for EK certificate fails; and

tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and

messaging said TPM vendors to update their security procedures.

17. A system for securely creating an endorsement certificate for a device in an insecure environment, said system comprising:

means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server;

means for verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufacture of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server; and

means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device wherein said inserting is completed only when said verifying step is confirmed.

18. The system of Claim 17, wherein said non-public, secure value is a secret number (secret) and said system further comprises means for forwarding a first copy of said secret via a secure communication medium to said credential server.

19. The system of Claim 18, further comprising:

means for hashing a second copy of said secret with a public key from said endorsement key pair;

means for combining a first hash result from said hashing step with the public key to create the endorsement key (EK); and

means for forwarding said EK to said credential server to initiate a credential process.

20. The system of Claim 19, said verifying means further comprising:

means for receiving said EK from said device at the credential server;

means for hashing the public key within the received EK with the first copy of said secret received during said forwarding step to provide a second hashed value;

means for comparing the first hashed value from within the EK with the second hash value; and

means for confirming said EK is from a valid device when said comparing step results in a match.

21. The system of Claim 17, wherein following said verifying said system further comprises:

means for initially storing the credential in a database of said credential server;

means for monitoring for a request from a customer to provide said certificate to said device; and

means for following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

22. The system of Claim 17, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said

device.

23. The system of Claim 17, wherein said value is injecting into said device, and said value is a single-use parameter, said system further comprising means for immediately destroying said value within said device following a creation of said EK.

24. The system of Claim 17, wherein said credential server is remotely located from a vendor manufacturing said device and said system comprises means for communicating said value from said device to said credential server via a secure communication medium.

25. The system of Claim 17, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined system for determining when to change said first value to said second value from among:

expiration of a pre-set amount of device manufacturing time; and

manufacture of a preset number of devices from among the plurality of valid devices.